

WHAT IS CLAIMED IS:

- 1 1. A method for encoding and decoding input data, comprising:
 - 2 (a) generating a key comprising a list of a plurality of binary values, wherein
 - 3 the key is made available to a user to enable decoding;
 - 4 (b) encoding the input data by:
 - 5 (i) using the key to initialize a replacement list;
 - 6 (ii) determining whether to replace strings in the input data with a
 - 7 string reference to a matching string value, wherein the input data not
 - 8 replaced with reference to one matching string values comprises one or more
 - 9 literals;
 - 10 (iii) replacing each literal with a literal reference to one entry in the
 - 11 replacement list matching the literal; and
 - 12 (c) decoding the encoded input data by:
 - 13 (i) accessing the generated key in response to user input; and
 - 14 (ii) using the accessed key to decode the literals replaced with literal
 - 15 references to entries in the replacement list.
 - 1 2. The method of claim 1, wherein the literal comprises a byte of the
 - 2 input data.
 - 1 3. The method of claim 1, wherein the user input comprises the generated
 - 2 key transferred by the user to the decoder.
 - 1 4. The method of claim 1, wherein the user input comprises a password,
 - 2 further comprising:
 - 3 using the password to generate the key used to initialize the replacement list
 - 4 during encoding.

1 5. The method of claim 1, wherein each string reference comprises a
2 copy pointer to a previous instance of the string in a history buffer generated while
3 scanning the input data.

1 6. The method of claim 1, wherein each string reference addresses one
2 entry in a compression dictionary comprising strings repeated in the input data.

1 7. The method of claim 1, wherein during encoding all the input data is
2 replaced with one string reference or literal reference.

1 8. The method of claim 1, wherein the replacement list includes 256
2 entries having every possible permutation of a byte.

1 9. The method of claim 1, wherein generating the key further comprises:
2 randomizing an order of the entries in the replacement list.

1 10. The method of claim 1, wherein the replacement list comprises a most
2 recently used (MRU) list, and wherein after replacing one literal with one literal
3 reference to one entry in the replacement list during encoding further performing:
4 promoting the entry matching the replaced literal to a first entry in the
5 replacement list.

1 11. The method of claim 1, wherein after replacing one literal with the
2 literal reference to one entry in the replacement list during encoding further
3 performing:
4 generating a pseudo random number; and
5 using the pseudo random number to determine whether to promote the entry
6 matching the replaced literal to a first entry in the replacement list.

1 12. The method of claim 1, wherein a first binary value is prepended to
2 each string reference in the encoded data and a second binary value is prepended to
3 the literal references in the encoded data.

1 13. The method of claim 12, wherein encoding the input data further
2 comprises:
3 generating a pseudo random number; and
4 using the generated pseudo random number to encrypt at least one prepended
5 first or second binary value.

1 14. The method of claim 1, wherein a first binary value is prepended to
2 each string reference in the encoded data and wherein one of a plurality of different
3 binary values is prepended to each literal reference in the encoded data, wherein each
4 of the plurality of binary values prepended to literal references corresponds to a
5 section of the replacement list and wherein the literal reference references one entry
6 in the section corresponding to the prepended binary value.

1 15. The method of claim 1, further comprising:
2 adding a number of bits from the encoded data plurality of the references to
3 either the matching string value in the input data or the replacement to one bit
4 package; and
5 for each bit package including, performing:
6 (i) generating a pseudo random number; and
7 (ii) using the generated pseudo random number to encrypt the bit
8 package including the encoded input data.

1 16. The method of claim 1, wherein encoding the input data further
2 comprises:
3 using at least one random number generator to generate random numbers to
4 encrypt the encoded input data; and
5 using the at least one random number generator to generate random numbers
6 to decrypt the encoded data.

1 17. A system for encoding and decoding input data, comprising:
2 (a) means for generating a key comprising a list of a plurality of binary values,
3 wherein the key is made available to a user to enable decoding;
4 (b) means for encoding the input data by:
5 (i) using the key to initialize a replacement list;
6 (ii) determining whether to replace strings in the input data with a
7 string reference to a matching string value, wherein the input data not
8 replaced with reference to one matching string values comprises one or more
9 literals;
10 (iii) replacing each literal with a literal reference to one entry in the
11 replacement list matching the literal; and
12 (c) means for decoding the encoded input data by:
13 (i) accessing the generated key in response to user input; and
14 (ii) using the accessed key to decode the literals replaced with literal
15 references to entries in the replacement list.

1 18. The system of claim 17, wherein the means for encoding the input data
2 further performs after replacing one literal with the literal reference to one entry in
3 the replacement list during encoding:
4 generating a pseudo random number; and

5 using the pseudo random number to determine whether to promote the entry
6 matching the replaced literal to a first entry in the replacement list.

1 19. The system of claim 17, wherein the means for encoding the input data
2 further performs prepending a first binary value to each string reference in the
3 encoded data and prepending a second binary value to the literal references in the
4 encoded data.

1 20. The system of claim 17, wherein encoding the input data further
2 performs:
3 using at least one random number generator to generate random numbers to
4 encrypt the encoded input data; and
5 using the at least one random number generator to generator random numbers
6 to decrypt the encoded data.

1 21. An article of manufacture including code for encoding and decoding
2 input data, wherein the code causes operations to be performed comprising:
3 (a) generating a key comprising a list of a plurality of binary values, wherein
4 the key is made available to a user to enable decoding;
5 (b) encoding the input data by:
6 (i) using the key to initialize a replacement list;
7 (ii) determining whether to replace strings in the input data with a
8 string reference to a matching string value, wherein the input data not
9 replaced with reference to one matching string values comprises one or more
10 literals;
11 (iii) replacing each literal with a literal reference to one entry in the
12 replacement list matching the literal; and
13 (c) decoding the encoded input data by:

14 (i) accessing the generated key in response to user input; and
15 (ii) using the accessed key to decode the literals replaced with literal
16 references to entries in the replacement list.

1 22. The article of manufacture of claim 21, wherein the literal comprises a
2 byte of the input data.

1 23. The article of manufacture of claim 21, wherein the user input
2 comprises the generated key transferred by the user to the decoder.

1 24. The article of manufacture of claim 21, wherein the user input
2 comprises a password, further comprising:
3 using the password to generate the key used to initialize the replacement list
4 during encoding.

1 25. The article of manufacture of claim 21, wherein each string reference
2 comprises a copy pointer to a previous instance of the string in a history buffer
3 generated while scanning the input data.

1 26. The article of manufacture of claim 21, wherein each string reference
2 addresses one entry in a compression dictionary comprising strings repeated in the
3 input data.

1 27. The article of manufacture of claim 21, wherein during encoding all
2 the input data is replaced with one string reference or literal reference.

1 28. The article of manufacture of claim 21, wherein the replacement list
2 includes 256 entries having every possible permutation of a byte.

1 29. The article of manufacture of claim 21, wherein generating the key
2 further comprises:
3 randomizing an order of the entries in the replacement list.

1 30. The article of manufacture of claim 21, wherein the replacement list
2 comprises a most recently used (MRU) list, and wherein after replacing one literal
3 with one literal reference to one entry in the replacement list during encoding further
4 performing:
5 promoting the entry matching the replaced literal to a first entry in the
6 replacement list.

1 31. The article of manufacture of claim 21, wherein after replacing one
2 literal with the literal reference to one entry in the replacement list during encoding
3 further performing:
4 generating a pseudo random number; and
5 using the pseudo random number to determine whether to promote the entry
6 matching the replaced literal to a first entry in the replacement list.

1 32. The article of manufacture of claim 21, wherein a first binary value is
2 prepended to each string reference in the encoded data and a second binary value is
3 prepended to the literal references in the encoded data.

1 33. The article of manufacture of claim 32, wherein encoding the input
2 data further comprises:
3 generating a pseudo random number; and
4 using the generated pseudo random number to encrypt at least one prepended
5 first or second binary value.

1 34. The article of manufacture of claim 21, wherein a first binary value is
2 prepended to each string reference in the encoded data and wherein one of a plurality
3 of different binary values is prepended to each literal reference in the encoded data,
4 wherein each of the plurality of binary values prepended to literal references
5 corresponds to a section of the replacement list and wherein the literal reference
6 references one entry in the section corresponding to the prepended binary value.

1 35. The article of manufacture of claim 21, further comprising:
2 adding a number of bits from the encoded data plurality of the references to
3 either the matching string value in the input data or the replacement to one bit
4 package; and
5 for each bit package including, performing:
6 (i) generating a pseudo random number; and
7 (ii) using the generated pseudo random number to encrypt the bit
8 package including the encoded input data.

1 36. The article of manufacture of claim 21, wherein encoding the input
2 data further comprises:
3 using at least one random number generator to generate random numbers to
4 encrypt the encoded input data; and
5 using the at least one random number generator to generator random numbers
6 to decrypt the encoded data.